

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA
v.
KENNETH UKHUEBOR and PATIENCE OSAGIE,
Defendants.

MEMORANDUM AND ORDER

20-MJ-1155 (LDH)

LASHANN DEARCY HALL, United States District Judge:

Defendants Kenneth Ukhuebor and Patience Osage move to quash the December 3, 2020 search warrant (the “Warrant”) issued by Magistrate Judge Bulsara as overbroad and lacking sufficient particularity with respect to electronic devices in violation of the Fourth Amendment.¹

BACKGROUND

On December 3, 2020, FBI Special Agent Alexander Turczak applied for the Warrant to arrest Defendants and search the premises located at 62-31 136th Street, Floor 2, Queens, New York 11367 (the “Premises”), submitting an affidavit in support of the application (the “Affidavit”). (Compl. Aff. Supp. Application Arrest Warrant Search Seizure Warrant (“Aff.”) ¶ 2, ECF 16-1.) The Affidavit alleges that Defendants Ukhuebor and Osage are married, reside at the Premises, and are affiliated with the company Kenbor, Inc. (Aff. ¶¶ 6-15.) Defendant Osage is listed as the person who should receive any legal process on behalf of Kenbor, Inc. on its business registration statement, and listed Kenbor, Inc. as her employer on social media. (*Id.* ¶¶ 7, 8, 11-12.) Based on links on social media, phone number registration overlap, and the fact that Kenbor appears to be a combination of Defendant Ukhuebor’s first and last name (Kenneth

¹ Defendants also moved to quash on Fifth Amendment grounds. However, the Government does not seek to enforce the provision of the search warrant at issue under the Fifth Amendment. (Gov’t Mem. L. Opp’n Defs.’ Mot. Quash (“Gov’t Opp’n”) 1, ECF No. 18.) Accordingly, that issue is now moot.

Ukhuebor), the Affidavit states that Defendant Ukhuebor is affiliated with Kenbor, Inc., through Defendant Osagie. (*Id.* ¶¶ 7-9, 13-15.) Defendant Osagie opened two bank accounts (the “8304 Account” and the “8113 Account”) on behalf of Kenbor, Inc., and Defendant Ukhuebor opened a third bank account on his own behalf (the “4690 Account”). (*Id.* ¶¶ 16-19.)

Defendants are alleged to have participated in two fraudulent schemes. The first was an advanced fee inheritance scheme, in which elderly victims were targeted and told that they were entitled to a large sum of money as the beneficiary of foreign estate, and will be paid the inheritance after the elderly victim makes a payment for taxes, fees, or other invented charges. (*Id.* ¶ 20.) One victim wrote a check for \$53,400 to Kenbor Inc. on December 18, 2018, which was deposited into the 8304 Account that same day. (*Id.* ¶ 21.) That victim communicated with a woman who held herself out as a Spanish bank manager through letters and faxes. (*Id.*) Cash was withdrawn from the 8304 Account in two withdrawals of \$30,000 and \$15,000 on December 19, 2018 and December 20, 2018, respectively. (*Id.* ¶ 26.) A second victim wired \$43,000 to the 4690 Account on July 18, 2019 after communicating with a purported London-based lawyer via a telephone call in March 2019 and via email on July 17, 2019. (*Id.* ¶ 22.) Between July 19 and July 24, 2019, over \$42,000 was withdrawn from the 4690 Account. (*Id.* ¶ 27.)

The second alleged scheme was a business compromise scheme. Through that scheme, the victim company (the “Victim Company”) received emails from a hacked email account of one of its vendors (the “Vendor Company”) in March and April 2020. (*Id.* ¶ 24.) On April 7, 2020, the Vendor Company emailed the Victim Company and requested future payments be made to the 8113 Account. (*Id.*) Ultimately, \$8,000,000 was wired to the 8113 Account from the Victim Company in April and May 2020. (*Id.*) More than \$900,000 of the proceeds drawn

on the 8113 Account between April and May 2020 were written out as checks, with the signature on the checks appearing to be Defendant Osagie's. (*Id.* ¶ 28.)

The Affidavit defined wire fraud, bank fraud, bank and wire fraud conspiracy, money laundering, and money laundering conspiracy as the “SUBJECT OFFENSES.” (*Id.* at 2.) In the Affidavit, Special Agent Turczak averred that based on his training and experience, he knew that “individuals who engage in wire fraud, bank fraud and money laundering activities commonly use phones, computers, or other electronic devices to access websites used for illegal activity, to communicate with victims and co-conspirators online, and to store records relating to transactions conducted as part of their illegal activities.” (*Id.* ¶ 35.) Special Agent Turczak further affirmed that individuals involved in such crimes “often store data on their computers related to their illegal activity, which can include logs of online chats with coconspirators; electronic communications with victims; contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social media accounts; and electronic records of financial transactions.” (*Id.*) Combined with the evidence detailed above, Special Agent Turczak stated that there was “probable cause to believe that phones and/or computer devices will be found on the [Premises] that contain evidence of the SUBJECT OFFENSES [and] to believe that these devices constitute instrumentalities and/or contraband subject to seizure, in that the devices were used to commit the SUBJECT OFFENSES.” (*Id.* ¶ 37.)

On December 3, 2020, United States Magistrate Judge Sanket J. Balsara issued the Warrant, authorizing law enforcement to search the Premises and to seize “evidence, contraband, fruits, or instrumentalities” of the SUBJECT OFFENSES for the time period from

November 1, 2018 to the present. (Warrant, Attachment B, ECF No. 16-2.) The Warrant defined the Subject Offenses as the same offenses listed in the Affidavit and defined evidence, contraband fruits, or instrumentalities to include:

Any phones, computers, or other electronic devices that reasonably appear to contain evidence of the above items or to be instrumentalities and/or contraband because they were used to commit the SUBJECT OFFENSES.

(*Id.*) The Warrant further stated that “the items to be seized do not include any phones, computers, or other electronic devices that reasonably appear to be within the exclusive possession or control of any individuals other than [Defendants].” On December 4, 2020, law enforcement arrested Defendants at the Premises and seized from the Premises six electronic devices: four Samsung cellular phones, an Apple iPhone and an Apple iPad. (*See* ECF No. 16-3.)

STANDARD OF REVIEW

The duty of a reviewing court is simply to ensure that the magistrate had a “substantial basis for concluding that probable cause existed.” *Illinois v. Gates*, 462 U.S. 213, 238-39 (1983) (internal modification omitted). A search warrant issued by a neutral and detached magistrate is entitled to substantial deference, and “doubts should be resolved in favor of upholding the warrant.” *United States v. Rosa*, 11 F.3d 315, 326 (2d Cir. 1993) (quoting *United States v. Travisano*, 724 F.2d 341, 345 (2d Cir.1983)).

DISCUSSION

I. Scope of Search Warrant

Defendants argue that the Warrant was overbroad as there was not sufficient nexus between the criminal activities alleged and the electronic items to be seized. (Def. Ukhuebor

Mem. L. Supp. Mot. Quash (“Ukhuebor Mem.”) 26, ECF 16; Def. Osagie Mem. L. Supp. Mot. Quash (“Osagie Mem.”) 9-10, ECF No. 17.) The Court disagrees.

In assessing whether there is probable cause to issue a warrant, the task of the issuing magistrate is to make a practical, common-sense decision that there is a fair probability that contraband or evidence of a crime will be found in a particular place. *Gates*, 462 U.S. at 238. In other words, “probable cause is a flexible common-sense standard,” *Texas v. Brown*, 460 U.S. 730, 742 (1983), “that does not deal with hard certainties, but with probabilities,” *Gates*, 462 U.S. at 231. Moreover, a showing of nexus between the alleged criminal activities and the place to be searched “does not require direct evidence and may be based on reasonable inference from the facts presented based on common sense and experience.” *United States v. Singh*, 390 F.3d 168, 182 (2d Cir. 2004).

Here, it was reasonable for the Magistrate Judge to find that that there was a fair probability that contraband or evidence of a crime would be found in electronic items belonging to Defendants on the Premises. As to Defendant Osagie, the Victim Company received an email on April 7, 2020 from the hacked account of the Vendor Company, requesting future payments be made to the 8113 Account, which was opened by Defendant Osagie. (*Id.* ¶ 24) Ultimately, \$8,000,000 was wired to the 8113 Account from the Victim Company in April and May 2020. (*Id.*) More than \$900,000 of the proceeds drawn on the 8113 Account between April and May 2020 were written out as checks, with the signature on the checks appearing to be Defendant Osagie’s. (*Id.* ¶ 28.) Given that Defendant Osagie was the owner of the 8113 Account, that the Victim Company received an email directing payments to be made to the 8113 Account, and it appears she signed the checks withdrawing the proceeds from those transfers, it was reasonable

for the Magistrate Judge to infer that there was a fair probability that electronic evidence of the crime would be found on Defendant Osagie's electronic devices.

As to Defendant Ukhuebor, one individual victim received an email from an individual named "Arne Zeidler" on July 17, 2019, instructing the victim to wire funds to the 4690 Account. (Aff. ¶ 22.) On July 18, 2019, that victim wired \$43,000 to the 4690 Account, which was an account opened by Defendant Ukhuebor. (*Id.*) Between July 19 and July 24, 2019, over \$42,000 was withdrawn from the 4690 Account. (*Id.* ¶ 27.) Against these facts, Defendant Ukhuebor argues that "the affidavit does not indicate any facts to suggest that . . . he sent that email." (Ukhuebor Reply Supp. Mot. Quash ("Ukhuebor Reply") 4, ECF No. 20.) He further argues that probable cause cannot be found without direct evidence tying the crime to an electronic device. (*Id.* 8.) To be sure, here, there is no direct evidence tying Defendant Ukhuebor to the email sent on July 17, 2019. However, that is not the standard. Probable cause does not require certainty, nor does it require direct evidence. *See Singh*, 390 F.3d at 182. Given that Defendant Ukhuebor was the owner of the 4690 Account and that an email was sent directing the wire transfer be made to the 4690 Account, it was reasonable for the Magistrate Judge to infer that there was a fair probability he was the sender of those emails. Or, in other words, that there was a fair probability that electronic evidence of the crime would be found on Defendant Ukhuebor's electronic devices.

Special Agent Turczak's expert opinion further supports the Magistrate Judge's finding of probable cause. Special Agent Turczak stated that based on his training and experience, he knew that "individuals who engage in wire fraud, bank fraud and money laundering activities commonly use phones, computers, or other electronic devices to access websites used for illegal activity, to communicate with victims and co-conspirators online, and to store records relating to

transactions conducted as part of their illegal activities. (Aff. ¶ 35.) Special Agent Turczak’s expert opinion “is an important factor to be considered in making a probable cause determination.” *United States v. Benevento*, 836 F.2d 60, 71 (2d Cir. 1987), *abrogated on other grounds by* *United States v. Indelicato*, 865 F.2d 1370 (2d Cir. 1989). To be sure, a government agent’s expert opinion, standing alone, might not be sufficient to establish a link between the item to be searched and the alleged criminal activity. *Id.* However, when viewed together with the other evidence in the Affidavit, it strengthens the Magistrate Judge’s finding of nexus. *See, e.g., United States v. Brown*, 676 F. Supp. 2d 220, 224, 228 (S.D.N.Y. 2009) (finding probable cause based on evidence of incriminating phone calls and the law enforcement affiant’s opinion that cellphones contained evidence of criminal activity based on his training and experience, coupled with the “commonsense notion” that an individual engaged in a conspiracy may have evidence of that conspiracy on communication devices used by the individual); *cf. United States v. Falso*, 544 F.3d 110, 124 (2d Cir. 2008) (finding that expert opinion of law enforcement coupled with unreasonable inferences did not support probable cause determination related to child pornography charges where there were no allegations that the defendant actually gained access to the website at issue, that the sole or principal purpose of the website was the viewing or sharing of child pornography, or that child pornography was downloadable from the site)).

Defendants’ cited caselaw in support of their motion to quash on lack of nexus grounds is distinguishable. In *United States v. Rutherford*, the affidavit before the Magistrate Judge merely proffered the “conclusory statement” that weapons in an apartment were unlawfully possessed, and there were no facts in the record that shed any light on whether the possession of the weapon was illegal. 71 F. Supp. 3d 386, 392 (S.D.N.Y. 2014). In light of this record, the court observed that “a conclusory legal allegation is insufficient to establish the existence of probable cause

sufficient to support the issuance of a search warrant.” *Id.*; *see also United States v. Guzman*, No. S5 97 CR 786 (SAS), 1998 WL 61850, at *4 (S.D.N.Y. Feb. 13, 1998) (“Permitting a search warrant based solely on the self-avowed expertise of a law-enforcement agent, without any other factual nexus to the subject property, would be an open invitation to vague warrants authorizing virtually automatic searches of any property used by a criminal suspect.” (internal quotations and citation omitted)). By way of contrast, here, as previously discussed, there were facts in the record—not just a single expert opinion by law enforcement—to support the reasonable inference that there was evidence of unlawful conduct on electronic devices located at the Premises.

United States v. Kortright likewise does not provide the court a basis to disturb the Magistrate Judge’s determination regarding probable cause. No. 10-CR-937, 2011 WL 4406352, at *7 (S.D.N.Y. Sept. 13, 2011). In *Kortright*, different from *Rutherford*, there was evidence of a criminal act—a handful of drug sales that occurred over a year prior in a location several miles from the residence. However, the only evidence that connected the place to be searched with the alleged criminal act was an opinion by a law enforcement officer that “drug traffickers typically keep evidence of their criminal activity in their residences.” *Id.* at *6-7. Ultimately, the *Kortright* court held that stale factual allegations of criminal activity over one year old, coupled with the expert opinion did not establish probable cause. *Id.*; *see also United States v. Griffith*, 867 F.3d 1265, 1274 (D.C. Cir. 2017) (holding that a affiant’s opinion based on experience that “gang members maintain regular contact with each other and often stay advised and share intelligence about their activities through cell phones and other electronic communication devices and the Internet” was insufficient to support a finding of probable cause where the police waited more than year since a shooting to seek a warrant). Here, the allegations of criminal

conduct are not stale as the alleged unlawful conduct occurred as recently as May 2020 and are not divorced from the electronic items to be searched and seized.

In sum, the Magistrate Judge's probable cause determination as to the nexus between the alleged crimes and the electronic items was not based on a finding that a cell phone is "inherently suspicious." (Ukhuebor Mem. 16; Osagie Mem. 11.) Rather, here, based on common sense, the Magistrate Judge properly determined that there was sufficient nexus between the alleged criminal activities and the electronic items to be searched and seized.²

II. Particularity

To satisfy the Fourth Amendment's particularity requirement, a warrant must: (1) identify the specific offense for which the police have established probable cause; (2) describe the place to be searched; and (3) specify the items to be seized by their relation to designated crimes.

United States v. Purcell, 967 F.3d 159, 178 (2d Cir. 2020). Defendants argue that the warrant lacks particularity in that it did not adequately identify places to be searched or items to be seized with respect to electronic devices and data. (Ukhuebor Mem. 30; Osagie 13-14.) The Court disagrees.

District courts in this circuit have found that a warrant that allows for the seizure of categories of materials may be impermissibly broad if such categories are not related to a specific individual, entity, offense, time frame, or other marker of relevance. *See, e.g., United States v. Zemlyansky*, 945 F. Supp. 2d 438, 457 (S.D.N.Y. 2013) (finding that a searched warrant that covered "[c]hecks, cash, and other financial instruments" without indicating any

² At best, Defendants' arguments and cited caselaw support an argument that the Magistrate Judge's probable cause finding was a close call. Even assuming that were true, doubts should be resolved in favor of upholding the warrant, and therefore the Court would still find the Affidavit established sufficient nexus to support a finding of probable cause.

individuals, entities, offenses, time frame, or relevance was impermissibly broad); *United States v. Wey*, 256 F. Supp. 3d 355, 385–87 (S.D.N.Y. 2017) (finding warrant failed to meet the particularity requirement where the warrant authorized seizure of a long list of materials such as, *inter alia*, financial records, notes, memoranda, records of internal and external communications, correspondence, audio tapes and video tapes, and photographs “regardless of their potential connection (or lack thereof) to any suspected criminal activities and limited only by the requirement that they relate in some generalized way to the owner/occupant of the very premises subject to search”).

In contrast, where, like here, items to be seized are defined by “reference to particular offenses and the use of an illustrative list,” courts in this Circuit have routinely upheld the warrant as sufficiently particularized. *United States v. Messalas*, No. 17-CR-339, 2020 WL 4003604, at *5 (E.D.N.Y. July 14, 2020) (collecting cases). In *United States v. Massalas*, for example, a search warrant defined items to be seized to include “all records relating to” violations of securities fraud, wire fraud, and money laundering statutes; “[r]ecords and information” relating to specified companies and entities; “[r]ecords relating to communications with co-conspirators”; and “any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant.” *Id.* at *1. Pursuant to the warrant, electronic devices were seized from the suspect’s home. *Id.* In upholding the validity of the search warrant on a motion to suppress, the *Messalas* court explained that “the particularity requirement is not usually interpreted to mean the officers must be left with no discretion whatsoever,” and there, the warrant was “sufficiently specific to permit the executing agents to exercise judgment in selecting what items to seize.” *Id.* at *5-6 (E.D.N.Y. July 14, 2020). Other courts in this district have upheld search warrants similar to the one in *Messalas*.

See, e.g., United States v. Chalavoutis, No. 18-CR-0349, 2019 WL 6467722, at *2 (E.D.N.Y. Dec. 2, 2019) (holding that warrant “passe[d] muster” despite broad scope, where a search of a defendant’s email account was by reference to the crimes investigated, the participants (unnamed co-conspirators), a time frame (6 years), and types of information and documents).

Here, the Warrant defined such evidence, contraband fruits, or instrumentalities to include:

Any phones, computers, or other electronic devices that reasonably appear to contain evidence of the above items or to be instrumentalities and/or contraband because they were used to commit the SUBJECT OFFENSES.

(Warrant, Attachment B.) The Warrant further stated that electronic devices to be seized did not include those that “reasonably appear to be within the exclusive possession or control of any individual other than [Defendants].” (*Id.*) And, the time frame was limited to November 1, 2018 to present, meaning that old electronic devices would not reasonably be subject to seizure. Defendants have cited to no case in which a warrant that limits the devices to be seized to a specific individual, crime, and time frame was found to be insufficiently particularized. Accordingly, the Court finds no basis to determine that the Warrant was insufficiently particular.

CONCLUSION

For the foregoing reasons, Defendants’ motions to quash the search warrant are DENIED.

SO ORDERED.

Dated: Brooklyn, New York
March 19, 2021

/s/ LDH
LASHANN DEARCY HALL
United States District Judge